CLAIMS

What is claimed is:

Sub a1

1. A method for integrating a digital signature service into a database, said method comprising the steps of:

receiving data, from a client of said database, for storage in a database record;

receiving a digital certificate for said client;

generating a signature from said data;

generating a signature object for said data, said digital signature object comprising said data, certificate and signature; and

storing said signature object as at least a portion of a record in said database.

2. The method as set forth in claim 1, further comprising the steps of:

receiving a query command from said user to retrieve said data from said record of said database table;

retrieving, in response to said query command, said data, certificate and signature for said user;

processing said data and said certificate, using said signature, to verify that said data and said certificate are unaltered from their original contents;

obtaining, from said certificate, an authentication as to the digital signatory; and

generating, as a response to said query command, said data, so as to

provide verification of said data with said signature and said certificate in response to said query.

3. The method as set forth in claim 2, further comprising the steps of:

receiving, as said query command, a query command to retrieve at least one record in said database comprising criteria based on digital signatures stored for said records;

identifying records in said database with said criteria regarding said digital signatures; and

retrieving said records identified in response to said query command.

4. The method as set forth in claim 3, further comprising the steps of:

extracting, from said records retrieved, data, certificate and signature stored in said record;

processing said data and said certificate, using said signature, to verify that said data and said certificate are unaltered from their original contents;

obtaining, from said certificate, an authentication as to the digital signatory of said data; and

generating, as a response to said query command, said data, so as to provide verification of said data with said signature and said certificate in response to said query.

5. The method as set forth in claim 1, wherein:

the step of generating a digital signature for said data comprises the step of generating a single signature object comprising said certificate, said document, and said digital signature; and

the step of storing said document, certificate and signature as at least a portion of a record in said database comprises the step of storing said single signature object in said record of said database.

6. The method as set forth in claim 5, wherein the step of generating a single signature object comprises the step of generating a serialized object comprising said certificate, said document, and said signature.

7. The method as set forth in claim 1, further comprising the step of storing said certificate of said user in a column of said database table.

8. The method as set forth in claim 7, wherein the step of storing said certificate of said user in a column of said database table comprises the step of augmenting a user identification field to include said certificate of said user.

9. The method as set forth in claim 1, further comprising the steps of:

receiving a second digital certificate for a second client;

retrieving said signature object from said record in said database as a first signature object;

generating a second signature from said first signature object with said second client as a signatory;

generating a second signature object, said second signature object comprising said first signature object, said second certificate, and said second signature; and

storing, in said database, said second signature object.

10. The method as set forth in claim 9, further comprising the steps of:

receiving a query command to retrieve said second signature object from said record of said database table;

retrieving, in response to said query command, said second signature object for said user;

processing said first signature object and said second certificate, using said second signature, to verify that said first signature object and said second certificate are unaltered from their original contents;

processing said data and said certificate, using said signature, to verify that said data and said certificate are unaltered from their original contents; and

generating, as a response to said query command, said data, so as to provide verification of said first and second digital signatures.

11. A computer readable medium comprising a plurality of instructions which, when executed by a computer, cause the computer to perform the steps of:

receiving data, from a client of said database, for storage in a database record;

receiving a digital certificate for said client;

generating a signature from said data;

generating a signature object for said data, said digital signature object comprising said data, certificate and signature; and

storing said signature object as at least a portion of a record in said database.

12. The computer readable medium as set forth in claim 11, further comprising the steps of:

receiving a query command from said user to retrieve said data from said record of said database table;

retrieving, in response to said query command, said data, certificate and signature for said user;

processing said data and said certificate, using said signature, to verify that said data and said certificate are unaltered from their original contents;

obtaining, from said certificate, an authentication as to the digital signatory; and

generating, as a response to said query command, said data, so as to provide verification of said data with said signature and said certificate in response to said query.

13. The computer readable medium as set forth in claim 12, further comprising the steps of:

receiving, as said query command, a query command to retrieve at least one record in said database comprising criteria based on digital signatures stored for said records;

identifying records in said database with said criteria regarding said digital signatures; and

retrieving said records identified in response to said query command.

14. The computer readable medium as set forth in claim 13, further comprising the steps of:

extracting, from said records retrieved, data, certificate and signature stored in said record;

processing said data and said certificate, using said signature, to verify that said data and said certificate are unaltered from their original contents;

obtaining, from said certificate, an authentication as to the digital signatory of said data; and

generating, as a response to said query command, said data, so as to provide verification of said data with said signature and said certificate in response to said query.

15. The computer readable medium as set forth in claim 11, wherein:

the step of generating a digital signature for said data comprises the step of generating a single signature object comprising said certificate, said document, and said digital signature; and

the step of storing said document, certificate and signature as at least a portion of a record in said database comprises the step of storing said single signature object in said record of said database.

16. The computer readable medium as set forth in claim 15, wherein

the step of generating a single signature object comprises the step of generating a serialized object comprising said certificate, said document, and said signature.

17. The computer readable medium as set forth in claim 11, further comprising the step of storing said certificate of said user in a column of said database table.

18. The computer readable medium as set forth in claim 17, wherein the step of storing said certificate of said user in a column of said database table comprises the step of augmenting a user identification field to include said certificate of said user.

19. The computer readable medium as set forth in claim 11, further comprising the steps of:

receiving a second digital certificate for a second client;

retrieving said signature object from said record in said database as a first signature object;

generating a second signature from said first signature object with said second client as a signatory;

generating a second signature object, said second signature object comprising said first signature object, said second certificate, and said second signature; and

storing, in said database, said second signature object.

20. The computer readable medium as set forth in claim 19, further comprising the steps of:

receiving a query command to retrieve said second signature object from said record of said database table;

retrieving, in response to said query command, said second signature object for said user;

processing said first signature object and said second certificate, using said second signature, to verify that said first signature object and said second certificate are unaltered from their original contents;

processing said data and said certificate, using said signature, to verify that said data and said certificate are unaltered from their original contents; and generating, as a response to said query command, said data, so as to provide verification of said first and second digital signatures.

21. A computer comprising:

an input device for receiving a digital certificate for a user of said computer;

database client for generating data for storage in a database record;

database management system, coupled to said database client, for generating a signature from said data, said database management system further for generating a signature object for said data, said digital signature object comprising said data, certificate and signature; and

database, coupled to said database management system, comprising a plurality of records for storing said signature object as at least a portion of a

record.